Determining Relationships in combined network privacy goals with formal automatic verification

Christiane Kuhn & Michael Kirsten

October 22, 2020

While encryption allows to protect the content of messages sent over the Internet, meta data (like who sends to whom) still leaks to Internet service providers and big companies. Such meta data is often enough to conclude wide-ranging private information about an individual. To protect meta data, anonymous communication networks [2], like Tor [1], and formal definitions to express their privacy protection were developed. The predominant approach to formalize the privacy protection is using indistinguishability games. In these an adversary is challenged to distinguish two cases. By defining how the compared cases are allowed to differ, different privacy goals can be expressed. Kuhn et al. [3] used this technique to define a large set of privacy goals and compared each goal to all others. Thereby, for each pair of goals it is shown if one is strictly stronger than the other, or if the goals are not directly related. This lead to a hierarchy of over 50 privacy goals.

However using this tool to assess the privacy of anonymous communication networks is easier, if more about the privacy goals and their relations to each other is known. While every single notion is already compared to all other notions, it is unclear what relations exist between sets of privacy notions. Further, understanding which additional relations exist under practical assumptions greatly helps researchers to understand privacy in this setting and to ease analysis of the protocols. Additionally the privacy goals can be extended with more useful goals.

Due to the many privacy goals, investigating all relationships between sets of them and all practical assumptions is infeasible to do by hand. Formal automatic verification, complemented with few cases that are checked by hand, makes the task manageable.

References

[1] Roger Dingledine, Nick Mathewson, and Paul Syverson. *Tor: The second-generation onion router*. Tech. rep. Naval Research Lab Washington DC, 2004.

[2] Matthew Edman and Bülent Yener. "On anonymity in an electronic society: A survey of anonymous communication systems". In: *ACM CSUR* (2009).

[3] Christiane Kuhn et al. "On Privacy Notion in Anonymous Communication". In: *PETs* (2019).